We claim:

1. An identification method, comprising:

detecting a distorted biometric for input into an identification system;

comparing the distorted biometric to one or more distortion patterns; and

determining an identity of the person based on results of said comparison.

2. The method of claim 1, wherein the biometric is an eye pattern.

3. The method of claim 2, wherein the detecting step includes:

detecting the eye pattern through a distortion element which generates the distorted biometric.

4. The method of claim 3, wherein the distortion element includes a lens having a non-linear optical pattern.

5. The method of claim 3, wherein the distortion element includes a diffraction grating which modulates the eye pattern to generate the distorted biometric.

6. The method of claim 5, wherein the diffraction grating is electronically generated adjacent to or within a lens.

7. The method of claim 3, wherein the detecting step includes:

acquiring the distorted biometric using an imaging system.

8. The method of claim 1, wherein the biometric is a fingerprint.

9. The method of claim 8, wherein the detecting step includes:

receiving a signal output from a distortion element which distorts the fingerprint.

10. The method of claim 9, wherein the distortion element includes a mask pattern.

11. The method of claim 10, wherein the mask pattern is superimposed over at least a portion of the fingerprint.

12. The method of claim 10, wherein the mask pattern does not obscure the fingerprint.

13. The method of claim 10, wherein the mask pattern is included in a window of a fingerpiece which fits over the person's finger.

14. The method of claim 10, wherein the mask patter is included on a medium placed over a fingerprint reader.

15. The method of claim 1, wherein the biometric is a palm print.

16. The method of claim 1, wherein the biometric is a voice of the person.

17. The method of claim 16, wherein the detecting step includes:

receiving a signal from a voice distortion unit which imposes a predetermined form of distortion on the voice of the person to generate the distorted biometric.

18. The method of claim 1, wherein the biometric is a handwriting sample.

19. The method of claim 17, wherein the detecting step includes:

receiving a signal from a reader which includes a mask pattern for distorting the handwriting sample.

20. The method of claim 1, wherein the biometric is a facial pattern.

21. The method of claim 20, wherein the detecting step includes:

detecting the facial pattern through a distortion element which generates the distorted biometric.

22. The method of claim 21, wherein the distortion element includes a lens having a non-linear optical pattern.

23. The method of claim 21, wherein the detecting step includes:

acquiring the distorted facial pattern using an imaging system.

24. The method of claim 21, wherein the distortion element includes a lens which distorts the facial pattern.

25. The method of claim 1, wherein the biometric is a DNA sample.

26. The method of claim 25, wherein the detecting step includes:

receiving an image of the DNA sample produced by a mask pattern.

27. The method of claim 1, wherein each of the distortion patterns corresponds to a distorted biometric of a respective one of a plurality of persons having a known identity.

28. The method of claim 27, wherein the distortion patterns are stored in a database.

29. The method of claim 27, wherein the distortion patterns are stored in a memory chip.

30. The method of claim 1, wherein the determining step includes:

determining the person has an unknown identity if no match results from the comparison.

31. The method of claim 1, wherein the distorted biometric is generated using a unique distortion element.

32. The method of claim 31, wherein the biometric is an eye pattern and the unique distortion element is a lens which distorts the eye pattern.

33. The method of claim 33, wherein the lens is included in an eyepiece carried by the person.

34. The method of claim 31, the biometric is a voice and the unique distortion element is a voice scrambler carried by the user.

35. An identification system, comprising:

a detector which captures a distorted biometric of a person; and

a processor which compares the distorted biometric to one or more distortion patterns and determines an identity of the person based on results of the comparison.

36. The system of claim 35, further comprising:

a distortion element which generates the distorted biometric of the person.

37. The system of claim 36, wherein the biometric is an eye pattern.

38. The system of claim 37, wherein the distortion element includes:

a lens having a non-linear optical pattern which generates a distortion of the eye pattern.

39. The system of claim 38, wherein the lens is included in an eyepiece carried by the person.

40. The system of claim 38, wherein the distortion element includes:

a diffraction grating which modulates the eye pattern to generate the distorted biometric.

41. The system of claim 40, wherein the diffraction grating is electronically generated adjacent to or within a lens.

42. The system of claim 38, further comprising:

a camera which captures the distorted eye pattern output from the distortion element.

43. The system of claim 36, wherein the biometric is a fingerprint.

44. The system of claim 43, wherein the distortion element includes:

a mask worn over the finger, said mask including a window which distorts the fingerprint to generate the distorted biometric.

45. The system of claim 36, wherein the biometric is a palm print.

46. The system of claim 36, wherein the biometric is a voice of the person.

47. The system of claim 46, wherein the distortion element includes:

a modulator which modulates a frequency signal with a voice signal from the person to generate the distorted biometric.

48. The system of claim 36, wherein the biometric is a handwriting sample.

49. The system of claim 48, wherein the distortion element includes:

a mask which distorts the handwriting sample.

50. The system of claim 36, wherein the biometric is a facial pattern.

51. The system of claim 50, wherein the distortion element includes:

a lens which generates a distorted image of the facial pattern.

52. The system of claim 36, wherein the biometric is a DNA sample.

53. The system of claim 52, wherein the distortion element includes:

a mask which isolates predetermined portions of the DNA sample to generate the distorted biometric.

54. The system of claim 36, wherein the distortion element has a non-linear distortion pattern.

55. The system of claim 35, wherein each of the distortion patterns corresponds to a distorted biometric of a respective one of a plurality of persons having a known identity.

56. The system of claim 55, further comprising:

a database for storing the distortion patterns.

57. The system of claim 55, further comprising:

a memory chip which stores the distortion patterns.

58. An identification method, comprising:

receiving a signal indicative of a combination of two or more unique identity attributes, at least one of the unique identity attributes corresponding to a biometric of a person;

comparing the signal to one or more identity patterns; and

determining an identity of a person based on results of said comparison.

59. The method of claim 58, wherein another one of the unique identity attributes is a predetermined distortion pattern, said signal indicative of a distortion of the biometric using the predetermined distortion pattern.

60. The method of claim 59, wherein the predetermined distortion pattern includes a non-linear distortion pattern.

61. The method of claim 58, wherein another one of the unique identity attributes is another biometric of the person, said signal indicative of a combination of the two biometrics.

62. The method of claim 58, wherein the biometric is one of an eye pattern, a fingerprint, a palm print, a voice, a handwriting sample, a face, and a DNA sample.

63. The method of claim 58, wherein said one or more identity patterns are stored in a database.

64. The method of claim 58, wherein said one or more identity patterns are stored in a memory chip.

65. The method of claim 58, wherein the determining step includes:

determining that the person is an unidentified person if no match occurs in the comparing step.

66. An identification system, comprising:

a receiver which receives a signal indicative of a combination of two or more unique identity attributes, at least one of the unique identity attributes corresponding to a biometric of a person; and

a processor which compares the signal to one or more identity patterns and determines an identity of a person based on results of said comparison.

67. The system of claim 66, wherein another one of the unique identity attributes is a predetermined distortion pattern, said signal indicative of a distortion of the biometric using the predetermined distortion pattern.

68. The system of claim 67, wherein the predetermined distortion pattern includes a non-linear distortion pattern.

69. The system of claim 66, wherein another one of the unique identity attributes is another biometric of the person, said signal indicative of a combination of the two biometrics.

70. The system of claim 66, wherein the biometric is one of an eye pattern, a fingerprint, a palm print, a voice, a handwriting sample, a face, and a DNA sample.

71. The system of claim 66, further comprising:

a database for storing said one or more identity patterns.

72. The system of claim 66, further comprising:

a memory chip which stores said one or more identity patterns.

73. The system of claim 66, wherein the processor determines that the person is an unidentified person if no match occurs in the comparing step.

74. The system of claim 66, further comprising:

a distortion pattern serving as another one of said unique identity elements.

75. The system of claim 74, wherein the distortion pattern includes a non-linear distortion pattern.

76. The system of claim 74, wherein said signal is indicative of distortion of the biometric using the distortion pattern.

77. A computer-readable medium including a program for performing an identification function, said program comprising:

a first code section for comparing a signal indicative of a combination of two or more unique identity attributes to one or more identity patterns, at least one of the unique identity attributes corresponding to a biometric of a person; and

a second code section for determining an identity of a person based on results of said comparison.

78. The computer-readable medium of claim 77, wherein another one of the unique identity attributes is a predetermined distortion pattern, said signal indicative of a distortion of the biometric using the predetermined distortion pattern.

79. The computer-readable medium of claim 78, wherein the predetermined distortion pattern includes a non-linear distortion pattern.

80. The computer-readable medium of claim 77, wherein another one of the unique identity attributes is another biometric of the person, said signal indicative of a combination of the two biometrics.

81. The computer-readable medium of claim 77, wherein the biometric is one of an eye pattern, a fingerprint, a palm print, a voice, a handwriting sample, a face, and a DNA sample.

82. The computer-readable medium of claim 77, wherein said one or more identity patterns are stored in a database.

83. The computer-readable medium of claim 77, wherein said one or more identity patterns are stored in a memory chip.

84. The computer-readable medium of claim 77, wherein the second code section determines that the person is an unidentified person if no match occurs in the comparing step.

85. The computer-readable medium of claim 77, wherein the medium is an optically readable medium.

86. The computer-readable medium of claim 77, wherein the medium is a magnetically readable medium.

87. The computer-readable medium of claim 77, wherein the medium is an integrated circuit chip.

88. A method for identifying a person, comprising:

generating an encoded biometric;

detecting the encoded biometric;

comparing the encoded biometric with a previously enrolled encoded biometric; and

determining an identity of a person based on a result of the comparison.

89. A system for identifying a person, comprising:

a detector which detects an encoded biometric; and

a processor which compares the encoded biometric with a previously enrolled encoded biometric and determining an identity of a person based on a result of the comparison.